TECHNISCHE UNIVERSITÄT DARMSTADT

Technische Universität Darmstadt
Department of Computer Science
Chair of Applied Cryptography

**Master Thesis**

# Incoercible Sale

**Longer subtitle (if required)**

Nikolaos Stivaktakis

September 26, 2019

Supervisors: Prof. Sebastian Faust, Ph.D.
2nd supervisor

## Abstract

Write an abstract

**!!! Prüfen Sie, dass der folgende Text aktuell ist (entsprechend der formalen Regeln des Studienbüros) !!!**
**!!! Check that this text is up to date (according to formal rules of the examination office) !!!**

## Erklärung zur Abschlussarbeit gemäß § 22 Abs. 7 APB TU Darmstadt

Hiermit versichere ich, **Nikolaos Stivaktakis**, die vorliegende Master-Thesis / Bachelor-Thesis gemäß § 22 Abs. 7 APB der TU Darmstadt ohne Hilfe Dritter und nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die Quellen entnommen wurden, sind als solche kenntlich gemacht worden. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.
Mir ist bekannt, dass im Falle eines Plagiats (§38 Abs.2 APB) ein Täuschungsversuch vorliegt, der dazu führt, dass die Arbeit mit 5,0 bewertet und damit ein Prüfungsversuch verbraucht wird. Abschlussarbeiten dürfen nur einmal wiederholt werden.
Bei einer Thesis des Fachbereichs Architektur entspricht die eingereichte elektronische Fassung dem vorgestellten Modell und den vorgelegten Plänen.

---

## English translation for information purposes only: Thesis Statement pursuant to § 22 paragraph 7 of APB TU Darmstadt

I herewith formally declare that I, **first name last name**, have written the submitted thesis independently pursuant to § 22 paragraph 7 of APB TU Darmstadt. I did not use any outside support except for the quoted literature and other sources mentioned in the paper. I clearly marked and separately listed all of the literature and all of the other sources which I employed when producing this academic work, either literally or in content. This thesis has not been handed in or published before in the same or similar form.
I am aware, that in case of an attempt at deception based on plagiarism (§38 Abs. 2 APB), the thesis would be graded with 5,0 and counted as one failed examination attempt. The thesis may only be repeated once.
For a thesis of the Department of Architecture, the submitted electronic version corresponds to the presented model and the submitted architectural plans.

---

Datum / Date

Unterschrift / Signature

# Contents

# 1 Introduction

# 2 Preliminaries

## 2.1 Cryptography

## 2.2 Game Theory

## 2.3 Blockchains

## 2.4 Smart Contracts

## 2.5 Escrows

# 3 Related work

## 3.1 first escrowless protocol

Zimbeck mit Bithalo auch die analyse erwähnen

## 3.2 digital vs Physical

Hier unbedingt Asganokar sein paper erwähnen (sale of digital goods)

# 4 Formalization

## 4.1 Entities

### 4.1.1 Seller

An entity that owns a specific physical good $G$. The seller has bigger utility in owning $P$ amount of coins in contrast to owning $G$. He therefore desires to exchange $G$ against coins of amount $P$.

### 4.1.2 Buyer

An entity that owns coins of at least amount of $P$. The Buyer has greater utility in owning $G$ in contrast to owning $P$ amount of coins. He therefore desires to exchange coins of amount $P$ against $G$.

### 4.1.3 Escrow/Smart Contract

An entity that should ensure that the trade is successful. It acts as a fully trusted oracle.

### 4.1.4 Helper Box

Fully trusted by Buyer. //need to expand on that

## 4.2 The Game

### 4.2.1 Start Point

A Seller and a buyer want to trade successfully: Both have funds in the given cryptocurrency. The seller is in possession of the physical good.

### 4.2.2 End Point

The buyer is in possession of the physical good and his funds have decreased by amount p. The funds of the seller have increased by p.

### 4.2.3 Assumptions

Both entities have access to the Escrow and know the addresses of each other. The seller also knows the physical address to which the buyer wants the good to be shipped. Other than this information they know nothing about each other.
Both parties can send funds in the given cryptocurrency to any address. The sender has the power to send/ship the physical good to any physical address he wants. The Escrow is a smart contract and both the seller and the buyer know the code of the Smart Contract.
We assume both entities to behave rational, meaning that they both want to maximise their expected payoff.
Transaction Fees and Fees for the escrows are not analysed.

### 4.2.4 Success of the trade

The trade is considered successful, if the situation transitions from the start point to the end point.

### 4.2.5 Goal

The goal is to design the Escrow in such a way, that it is the best strategy for both the buyer and the seller to perform a successful trade. That means that a successful trade should be the Nash Equilibrium.

# 5 Proposed Possible Solutions

## 5.1 The naive approach

To examine any possible solutions, we begin with the simplest possible protocol.
The simplest protocol is the following: The seller ships the physical good $G$ to the provided address and the buyer sends coins of amount $P$ to the seller. There is no third party involved.

#### Payout

To analyze the payout for each party and each strategy I will use a table.

#### Example table

| | $H_B$ | -$H_B$ |
|---|---|---|
| $H_S$ | $P_S \vert P_B$ | $P_S \vert P_B$ |
| -$H_S$ | $P_S \vert P_B$ | $P_S \vert P_B$ |

#### Description

On the top are the possible strategies for the buyer: $H_B$ is the strategy where the buyer behaves honestly and -$H_B$ is the strategy where the Buyer behaves dishonestly.
On the left side are the strategies for the seller. Similar to the buyer, $H_S$ denotes the strategy where the seller behaves honestly and -$H_S$ denotes the strategy where the seller behaves dishonestly.

For each combination of strategies the two parties get a specific payout. $P_S$ denotes the payoff of the seller and $P_B$ denotes the payoff of the buyer.
This protocol has an obvious downside: There is no incentive for the seller to ship the good as well as for the buyer to send the coins.

#### Payout for the naive approach

| | $H_B$ | -$H_B$ |
|---|---|---|
| $H_S$ | $P \vert G$ | $0 \vert P+G$ |
| -$H_S$ | $P+G \vert 0$ | $G \vert P$ |

If we look at the payoff table we can see that -$H_B$ dominates $H_B$ and -$H_S$ dominates $H_S$. This means that the dishonest strategy provides a bigger payoff regardless of the strategy of the other party.
Since we assume the players to be rational, they would both chose the dishonest strategy. Both players chosing the dishonest strategy is the Nash Equilibrium of the game.
It is interesting to note that this table resembles the famous prisoner's dilemma. The Nash Equilibrium is on both parties not sending anything, still it would be better for both parties if they just traded honestly. Nothe that utility of P and utility of G

## 5.2 One Side collateral

To incentivize an entity to behave honestly we introduce collateral. The collateral will be lost, if the entity does not behave honestly. In this section I will look at protocols, where only one entity deposits a collateral.

### 5.2.1 Buyer Collateral

Following protocol is proposed:

1. Buyer deposits collateral $C > P$ to the Smart Contract
2. Seller sends physical good $G$ to the seller
3. After receiving $G$, the Buyer sends funds of amount $P$ to the seller
4. The Smart Contract releases the collateral of the Buyer

Because the Smart Contract has access to the blockchain, it can automatically release the collateral if the Buyer sends $P$ to the seller. The collateral should incentivize the Buyer to pay the seller after receiving the physical good $G$.

#### Possible Strategies

With this new protocol there are new possible strategies. Of course there is still the honest strategy for both players, where they behave according to the protocol description. With this strategy the trade unravels successfully.
But there exist other strategies: The dishonest strategy is again not sending the resources. This strategy is denoted as -$H_B$ (when the buyer does not send the coins) and -$H_S$ (when the seller does not send the physical good.
The Seller has also a third possible strategy: Since he decides what happens to the collateral, he can coerce the Buyer into sending him extra resources. This strategy will be denoted $C_S$. When the seller uses strategy $C_S$, he does not send the physical good. He rather sends a message to the Buyer: "I will not send you the physical good. Since your collateral is locked and it will only be released if you pay me $P$, I propose the following deal: In spite of me not sending you $G$, you still send me P and you get back your collateral. In addition I will send you $\frac{P}{2}$ back."

#### Payout

| | $H_B$ | -$H_B$ |
|---|---|---|
| $H_S$ | $P\|G$ | $0\|G+P-C$ |
| -$H_S$ | $G\|P-C$ | $G\|P-C$ |
| $C_S$ | $G\|P-C$ | $G+\frac{P}{2}\|\frac{P}{2}$ |

The biggest possible payout for the Seller is if he can coerce the Buyer into sending him additional $\frac{P}{2}$ coins. This happens when the seller is choosing strategy $C_S$ and the buyer strategy -$H_B$. It should be noted, that when the seller tries to coerce the buyer ($C_S$), it is actually his best option to comply (-$H_B$). This scenario is the Nash Equilibrium, because choosing a different strategy only results in a lower payoff for the player, if the other player is keeping his strategy.
The Nash Equilibrium would result in a payoff of $G+\frac{P}{2}$ for the Buyer and a payoff of $\frac{P}{2}$ for the seller. The rational buyer would never initiate the trade, because this trade will always result in a loss, if the seller behaves rational.

### 5.2.2 Seller Collateral

Following protocol is proposed:

1. Seller deposits collateral $C > P$ to the Smart Contract
2. Buyer sends funds of amount $P$ to the seller
3. Seller sends the physical good to the Buyer
4. Buyer receives the physical good and confirms it to the Smart Contract

5. The Smart Contract releases the collateral of the Seller

The collateral should incentivize the Seller to behave honestly and to ship the physical good to the buyer.

**Possible Strategies**

With this new protocol there are again new possible strategies. There is still the honest strategy for both players, where they behave according to the protocol description. With this strategy, the trade still unravels successfully.
But there exist other strategies: The dishonest strategy is again not sending the resources. This strategy is still denoted as -$H_B$ (when the buyer does not send the coins) and -$H_S$ (when the seller does not send the physical good.
The Buyer has also a unique opportunity: Since he decides what happens to the collateral, he can coerce the Seller into sending him extra resources. This strategy will be denoted $C_B$. After receiving the physical good he can tell the Seller: "Either you send me $\frac{C}{2}$ extra coins or I will tell the Smart Contract that you did not send me the physical good." In this case it is best for S to comply, because getting half his collateral back is better than losing it all.

**Payout**

| | $H_B$ | -$H_B$ | $C_B$ |
|---|---|---|---|
| $H_S$ | $P\|G$ | $G\|P$ | $P-\frac{C}{2}\|G+\frac{C}{2}$ |
| -$H_S$ | $P+G-c\|0$ | $G\|P$ | $G+P-\frac{C}{2}\|\frac{C}{2}$ |

If B sends the coins (does not choose strategy -$H_B$), S has to make the following decision: Does he send the good ($H_S$) or not (-$H_S$)? We have to take into account, that B decides what happens with the collateral.
What was designed to be an incentive for S to behave honestly, ended up as leverage for B over S. B can report 0 (and burn the collateral) even if S behaves honestly. Since sending the good has no impact on the collateral (the rational buyer will always play strategy $C_B$ over $H_B$), it is best for S to not send the physical good (-$H_B$). Because not Sending (-$H_S$) is the best strategy for the seller, it is best for B to not even send P and therefore not engage in the trade at all (-$H_B$).
The Nash Equilibrium would be in nobody sending anything and the trade not happening.

$$U_s(P) > U_s(nothing) \tag{5.1}$$

# 6 Open Research/ Questions

# 7 Conclusion